

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

UNITED STATES OF AMERICA,	)	
	)	
v.	)	CASE NO. 1:17-CR-292-ELR-AJB
	)	
ARTURO GONZALEZ-RENTERIA,	)	
Defendant.	)	

**DEFENDANT’S FIRST PARTICULARIZED MOTION TO SUPPRESS  
EVIDENCE AND BRIEF IN SUPPORT “PART II”, RE: MOTION TO SUPPRESS  
EVIDENCE AND STATEMENTS ILLEGALLY SEIZED PURSUANT TO TITLE III  
WIRETAP ORDERS AND ROVING WIRETAP INTERCEPTION  
AND FOR *FRANKS* HEARING**

COMES NOW the Defendant, Arturo Gonzalez-Renteria (hereinafter “Gonzalez” or “Defendant”), by and through undersigned counsel, pursuant to Fed.R.Crim.P. 12(b)(3)(C), and moves this Court for 1) an evidentiary hearing, 2) an order suppressing all evidence of any kind and the fruits thereof— including alleged physical evidence, statements, identification, and testimony—illegally seized by law enforcement agents in violation of Defendant’s First, Fourth, Fifth, Sixth or Fourteenth Amendment rights, 18 USC 2234, 18 USC 2510, et seq., or Fed.R.Crim.P. 41, during and subsequent to the illegal wiretaps of Defendant’s telephone communications, and 3) a *Franks* hearing as to whether the Government deliberately misled the issuing court in its applications for wiretaps and “roving” wiretaps pursuant to 18 USC 2515(11)(b).

**I. MOTION TO SUPPRESS INTERCEPTED COMMUNICATIONS**

Pursuant to the Fourth Amendment to the United States Constitution and 18 USC 2515 and 2518, Defendant moves this Court to suppress any and all evidence obtained through intercepted wire, electronic, and/or oral communications. As grounds thereof, Defendant alleges that the Title III wiretaps and the roving wiretap interceptions were improper, illegal, and

without probable cause, in violation of Defendant's rights under the Fourth, Fifth, and Fourteenth Amendments to the United States Constitution in the following particulars:

#### **A. Standing**

Movant has standing to contest the legality of any and all interceptions of his wire/oral/electronic communications in that Movant is an "aggrieved" person pursuant to 18 USC 2510 *et seq.*, particularly 18 USC 2518(10)(a), in that 1) he and his phone/communications were unlawfully intercepted during the interception of Target Telephones ("TT") 13, 15, 17, 5635 phone (17a), 2847 phone (17b), telephones belonging to Defendant Gonzalez-Renteria, 2) the order of authorization or approval under which they were intercepted are insufficient on their face, and 3) the interceptions were not made in conformity with the order of authorization or approval. *See, e.g.* H.Rep. No.1549, 91st Cong. 2<sup>nd</sup> Sess., *United States v. Tucker*, 526 F.2d 279, 282 & n. 4 (5<sup>th</sup> Cir. 1976) (a cognizable "claim" need be no more than a "mere assertion" provided that it is a positive statement that unlawful surveillance has taken place; court contrasts this with the situation where a movant only alleges they "may have" been illegally intercepted); *United States v. Pacella*, 622 F.2d 640 (2d Cir. 1980); *United States v. Williams*, 580 F.2d 578 (D.C. Cir. 1978).

#### **B. Statutory Framework and Requirements of Interception of Private Communications**

The fundamental framework behind all wiretapping statutes, whether state or federal, is the protection of privacy rights of citizens from unwarranted invasions by government (or private) intrusions. To protect that "fundamental" right, both federal and state governments have erected statutory barriers to the interception of presumptively private conversations.

To that end, in 1968 Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC 2510-2521) to conform to the constitutional standards governing

wiretaps prescribed by the Supreme Court in *Berger v. New York*, 388 U.S. 41(1967), and *Katz v. United States*, 389 U.S. 347 (1967). That Act, as amended, requires (at a minimum) the following: a full and complete statement of the alleged offense, the facilities where the communications are to be intercepted, a particular description of the communications sought to be intercepted, the identity of the persons committing the offense and of persons whose communications are to be intercepted, a full and complete statement of whether or not other investigative procedures have been tried and failed or why they appear unlikely to succeed or are too dangerous, and a full and complete statement of the period of time for which the interception is to be maintained. *See, e.g.* 18 USC 2518(1)(c) and (3)(c), *United States v. Kahn*, 415 U.S. 143, 153 n. 12(1974); *United States v. Giordano*, 416 U.S. 505 (1974). Additionally, any application must include information concerning previous applications involving any of the same persons, facilities or places. 18 USC 2518(1)(e).

If presented with an appropriate application, a court may actually issue a surveillance order for interception of private communications only if it finds probable cause<sup>1</sup> to believe that (1) a person is committing one of the crimes enumerated in section 2516 of Title III; (2) communications concerning such an offense will be obtained through interception, (3) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous, and (4) the facilities from which the communications which are to be intercepted are being used in connection with the commission of the offense. 18 USC 2518(3)(a), (b), (c) and (d).<sup>2</sup>

---

<sup>1</sup> The probable cause standard is the same as that used in ordinary search warrants, *see, United States v. Green*, 40 F.3d 1167 (11<sup>th</sup> Cir. 1994); *United States v. Wagner*, 989 F.2d 69, 71 (2<sup>nd</sup> Cir. 1993).

<sup>2</sup> Of course, the court must find that investigative techniques have failed.

If the above is met, a court may issue an order which specifies the identity of the person whose communications are to be intercepted, 18 USC 2518(4)(a), and the nature and location of the communications facilities or the place where the interception will occur. 18 USC 2518(b). The order must also specify the type of communication to be intercepted, the particular crime to which it relates, and length of authorized interception. 18 USC 2518(4)(c) and (e).

The order itself must be executed “as soon as practicable” and “terminate upon attainment of the authorized objective.” 18 USC 2518(5). Periodic progress reports may also be required by order of the court. *See*, 18 USC 2518(6); *United States v. Van Horn*, 789 F.2d 1492, 1499 (11<sup>th</sup> Cir. 1986).

Post-authorization duties attendant to the execution of an interception warrant include, *inter alia*, minimization,<sup>3</sup> and timely sealing.<sup>4</sup>

Finally, Title III must be strictly construed in favor of privacy interests because Congress intended Title III's procedural controls to be a “pre-condition to the acceptability of any wiretapping at all.”

Title III also contains a “necessity” requirement, separate and distinct from any probable cause requirement that must be satisfied before a wiretap order may be lawfully issued. 18 USC 2518(1)(c), 2518(3)(c). The purpose of the necessity requirement is “to ensure that the relatively intrusive device of wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime.” *United States v. Edwards*, 69 F.3d 419,429 (10<sup>th</sup> Cir. 1995) quoting *United States v. Kahn*, 415 U.S. 143,153 n.12(1974). Thus, before issuing a

---

<sup>3</sup> 18 USC 2518(5); *United States v. Moody*, 977 F.2d 1425 (11<sup>th</sup> Cir. 1992).

<sup>4</sup> 18 USC 2518(8)(a) and (b); *United States v. Matthews*, 431 F.3d 1296 (11<sup>th</sup> Cir. 2005); *United States v. Ojeda Rios*, 495 U.S. 257 (1990).

wiretap order, a court must independently determine that the requested wiretap is necessary. *See, e.g., United States v. Mondragon*, 52 F.3d 291, 293 (10<sup>th</sup> Cir. 1995).

To meet this burden, “generalities, or statements in the conclusory language of the statute, are insufficient to support a wiretap application.” *United States v. Castillo-Garcia*, 117 F.3d 1179, 1188 (10<sup>th</sup> Cir. 1997). In *United States v. Blackmon*, 273 F.3d 1204 (C.A. 9<sup>th</sup> Cir. 2001), the Court held that a wiretap application is insufficient where it contains “only general allegations that would be true in most narcotics investigations . . . [and] boilerplate conclusions that merely describe inherent limitations of normal investigative procedures.” *Id.* at 1210.

In fact, “[T]he statements must be factual in nature and they must specifically relate to the individuals targeted by the wiretap.” *Id. See also United States v. Smith*, 31 F.3d 1294 (4<sup>th</sup> Cir. 1994); *United States v. Ashley*, 876 F.2d 1069, 1072 (1<sup>st</sup> Cir. 1989) (“bare conclusory statements”); *United States v. Leavis*, 853 F.2d 215 (4<sup>th</sup> Cir. 1988); *United States v. McKinney*, 785 F.Supp. 1214 (D. Md. 1992); *United States v. Ippolito*, 774 F.2d 1482 (9<sup>th</sup> Cir. 1985); *United States v. Robinson*, 698 F.2d 448 (D.C. Cir. 1983); *United States v. Kalustian*, 529 F.2d 585 (9<sup>th</sup> Cir. 1976).

Similarly, the adoption of the exact language from prior applications fails to satisfy the congressional intent that the government must show with specificity in each application why it will fail in lieu of a wiretap order. *See Castillo-Garcia, supra. See also, United States v. Simpson*, 813 F.2d 1462, 1471-1472 (9<sup>th</sup> Cir. 1987); *United States v. Carneiro*, 861 F.2d 1171, 1176 (9<sup>th</sup> Cir. 1988).

That is, identity between applications indicates that the government “never paused to give further renewed consideration of...normal investigative procedures...and it never really tried to use any of these procedures...(and the government) proceeded from one wiretap to another.”

*United States v. Castillo-Garcia*, 920 F.Supp. 1537,1543 (D.Colo. 1996) aff'd 117 F.3d 1179 (10<sup>th</sup> Cir. 1997). Thus, in order to obtain an electronic surveillance order, the government must move beyond “bare conclusory statements” *Ashley, supra*, or “mere boilerplate recitations,” *Leavis, supra*, “to explain fully... with particularity”, *Castillo-Garcia*, why specific techniques would either be unsuccessful or too dangerous.

With regard to minimization, section 2518(5) requires each initial and extension order to include a minimization requirement. *See Scott v. United States*, 436 U.S. 128 (1978). Minimization embodies the constitutional requirement of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated, and limiting the scope of any invasion of privacy by the government. *See Berger v. New York*, 388 U.S. 41 (1967). To accomplish minimization, the most effective form of supervision is judicial review of the progress. *See United States v. Quintana*, 508 F.2d 867 (7<sup>th</sup> Cir. 1975); Section 2518(6). Courts have also approved a "two-minute" rule, *see, e.g. United States v. Moody*, 762 F.Supp. 1491, 1497 (N.D. Ga. 1991), to determine the pertinence of the conversation.<sup>5</sup>

If intercepted communications are in code or a foreign language, and an expert in that foreign language or code is not present during the interception period, minimization may be accomplished as soon as practicable after such interception. 18 USC 2518(5). Thus, if foreign language expert monitors were not available during the interception period, the government has the burden of showing that the government made immediate reasonable efforts to have such monitors available during the interception period, and that despite these reasonable efforts, the monitors were unavailable, and, that after-the-fact minimization by these monitors was accomplished as soon as practicable and in a reasonable manner. *United States v. Padilla-Pena*,

---

<sup>5</sup> Although after surveillance has been underway for some period, two minutes for determining pertinence is too long. *See United States v. Parks*, 1997 WL 136761, at 18 (N.D.Ill. 1997).

129 F.3d 457, 463 (8<sup>th</sup> 1997)(after-the-fact minimization allowed because government believed pertinent calls would be in English and had not procured Spanish speaking monitors before activating wiretap, thus, Spanish monitors were not “readily available” at inception of the wiretap; also, government obtained translators as soon as possible after-the-fact, and, within two weeks had full-time monitors who could translate and conduct immediate minimization); *See United States v. Castillo Garcia*, 920 F.Supp. 1537, 1552 (1996)(government showed Spanish monitor utilized and present during all intercepted communications).

Because Movant contends that insufficient minimization procedures were utilized *sub judice*, the burden is on the government to show proper minimization. *United States v. Torres*, 908 F.2d 1417 (9<sup>th</sup> Cir. 1990); *United States v. Armocida*, 515 F.2d 29 (3<sup>rd</sup> Cir. 1975); *United States v. Rizzo*, 491 F.2d 215, 217, n.7 (2<sup>nd</sup> Cir. 1974).

In order to fully litigate this issue, Movant requests a hearing at which the government must bear the burden of proof as to, *inter alia*:

- a. The number and identification of intercepted conversations which were “coded” and the efforts and techniques utilized to “decode” such conversations either at the time or after the conversation;
- b. How soon after the termination of any conversation the minimization occurred, including conversation in a foreign language; and
- c. Who accomplished the minimization and whether they were an expert in foreign or code language.

Further, to obtain “roving” surveillance of wire and electronic communications, as was done in this case for certain phones, law enforcement were required to meet certain heightened

standards under 18 USC 2518(11)(a), which only permits a roving wiretap in very narrow situations, by authorization from a court sitting with the requisite jurisdiction over the phones.

### **C. Grounds for Suppression of Wiretaps**

Defendant moves, pursuant to Fed.R.Crim.P. 12(b)(3) and 41(f), 18 USC 2515 and 2518(10)(a) and the Fourth Amendment to the United States Constitution to suppress the contents of any wire, electronic, and/or oral communication intercepted pursuant to a court order described below and any evidence derived therefrom on the grounds that:

- a. The communications were unlawfully intercepted;
- b. The orders of authorization were insufficient on their face;
- c. The applications and court orders were obtained in violation of 18 USC 2510 *et seq.*, including 18 USC 2515 and 2518; and
- d. The interceptions were not made in conformity with the court order or with the requisites of 18 USC 2518.

Movant alleges the following grounds in support of this motion and reserves the right to supplement this motion in writing or *ore tenus* upon receipt of any additional documents reflecting on the matters herein.

### **D. The Illegal Wiretap Orders & Roving Wiretap Interceptions**

Law enforcement obtained both Title III Wiretap orders and alleged “roving” wiretaps for numerous telephones (TT#1-TT#19), as well as extension orders, in which Defendant’s wire and electronic communications were captured. Wiretaps were issued for the following telephones:

#### **1) Interceptions of others’ telephones**

1. October 25, 2016 – 1:16-MJ-882
  - a. TT#1 (PIN D3F5B84F)<sup>6</sup> (Original) (Servicio);
2. November 21, 2016- 1:16-MJ-950

---

<sup>6</sup> The interception of “PIN” identifications relates to the interception of Blackberry electronic communications occurring on Blackberry phones.

- a. TT#1 (PIN D3F5B84F) (1<sup>st</sup> Cont.) (Servicio);
  - b. TT#2 (PIN D1B516D3) (Original) (Tommy Gun);
  - c. TT#3 (PIN 299CA827)(Original) (Positivo);
- 3. December 19, 2016 – 1:16-MJ-1027
  - a. TT#1 (PIN D3F5B84F) (2<sup>nd</sup> Cont.) (Servicio);
  - b. TT#2 (PIN D1B516D3) (1<sup>st</sup> Cont.) (Tommy Gun);
  - c. TT#3 (PIN 299CA827)(1<sup>st</sup> Cont.) (Positivo);
- 4. January 17, 2017 – 1:17-MJ-25
  - a. TT#1 (PIN D3F5B84F) (3rd Cont.) (Servicio);
  - b. TT#2 (PIN D1B516D3) (2nd Cont.) (Tommy Gun);
  - c. TT#4 (PIN 7ADO4A75) (Original) (Piter);
  - d. TT#5 (PIN 2B78D30F) (Original) (Positivo);
- 5. February 14, 2017 – 1:17-MJ-101
  - a. TT#1 (PIN D3F5B84F) (4th Cont.) (Servicio);
  - b. TT#2 (PIN D1B516D3) (3<sup>rd</sup> Cont.) (Tommy Gun);
  - c. TT#5 (PIN 2B78D30F) (1<sup>st</sup> Cont.) (Positivo);
  - d. TT#6 (PIN 2C30347E) (Original) (Primo Siempre);
  - e. TT#7 (PIN D8AAED8D) (Original) (Piter);
- 6. March 14, 2017 – 1:17-MJ-176
  - a. TT#2 (PIN D1B516D3) (4<sup>th</sup> Cont.) (Tommy Gun);
  - b. TT#5 (PIN 2B78D30F) (2<sup>nd</sup> Cont.) (Positivo);
  - c. TT#6 (PIN 2C30347E) (1<sup>st</sup> Cont.) (Primo Siempre);
  - d. TT#7 (PIN D8AAED8D) (1<sup>st</sup> Cont.) (Piter);
- 7. April 11, 2017 – 1:17-MJ-261
  - a. TT#6 (PIN 2C30347E) (2<sup>nd</sup> Cont.) (Primo Siempre);
  - b. TT#7 (PIN D8AAED8D) (2<sup>nd</sup> Cont.) (Piter);
  - c. TT#8 (PIN 2825668D) (Original) (Fede);
  - d. TT#9 (PIN 569460F) (Original) (Porteraso);
  - e. TT#10 (PIN 25B209DB) (Original) (Emperador);
- 8. May 10, 2017 – 1:17-MJ-384
  - a. TT#7 (PIN D8AAED8D) (3<sup>rd</sup> Cont.) (Piter);
  - b. TT#8 (PIN 2825668D) (1<sup>st</sup> Cont.) (Fede);
  - c. TT#10 (PIN 25B209DB) (1<sup>st</sup> Cont.) (Emperador);
  - d. TT#11 (PIN D8AE0799) (Original) (Primo Siempre);
  - e. TT#12 (PIN D8DF012A) (Original) (Rolex);
- 9. June 9, 2017 – 1:17-MJ-474
  - a. TT#11(1<sup>st</sup> Cont.)<sup>7</sup>
- 10. July 13, 2017 – 1:17-MJ-584
  - a. TT#11 (PIN D8AE0799) (2<sup>nd</sup> Cont.) (Primo Siempre);
  - b. TT#14 (PIN 2B84AB6E) (1<sup>st</sup> Cont.) (Emperador);

---

<sup>7</sup> Discovery appears to be incomplete. Defendant does not have discovery of the 17-MJ-474 order, but has two sealing applications and orders describing interception of TT#11 from June 9, 2017 to July 8, 2017, and sealed on July 10, 2017. (WIRE-17MJ0474-000195, n. 1) Defendant therefore reserves the right to amend this motion in writing or *ore tenus* before the Court upon receipt of this discovery.

- c. TT#16 (PIN D8ED87BC) (1<sup>st</sup> Cont.) (Nueve);
- d. TT#18 (PIN 2B7A1631) (Original) (Aguila);
- 11. August 15, 2017 – 1:17-MJ-681
  - a. TT#11 (PIN D8AE0799) (3<sup>rd</sup> Cont.) (Primo Siempre);
  - b. TT#19 (PIN D8A49EBB) (Original) (Emperador).
- 12. June 9, 2017 – 1:17-MJ-474
  - a. TT#11 (PIN D8AE0799) (1<sup>st</sup> Cont.) (Primo Siempre);
  - b. TT#14 (PIN 2B84AB6E) (Original) (Emperador);
  - c. **TT#15 (903-245-8658) (Original) (Gonzalez-Renteria)** (see below)
  - d. TT#16 (PIN D8ED87BC) (Original) (Nueve)

**2) Interceptions for Defendant Gonzalez-Renteria's telephones:**

**1. May 31, 2017 – 1:17-MJ-438**

- a. **TT#13 (470-595-5670) (Original) (Gonzalez-Renteria)**
  - i. Interception Period: June 3, 2017 to June 14, 2017
  - ii. Return: June 15, 2017 (see below)
  - iii. Sealing Order: June 15, 2017

**2. June 9, 2017 – 1:17-MJ-474**

- a. **TT#15 (903-245-8658) (Original) (Gonzalez-Renteria)**
  - i. Interception Period: June 10, 2017 to June 14, 2017
  - ii. Return: **TT13** and **TT15** on June 15, 2017
  - iii. Sealing Order: June 15, 2017

**3. June 28, 2017 – 1:17-MJ-529**

- a. **TT#17 (470-449-5260) (Original) (Gonzalez-Renteria);**
  - i. Interception Period: June 29, 2017 to July 13, 2017
  - ii. Return: July 13, 2017
  - iii. Sealing Order: July 14, 2017 (App 7/14/17: WIRE-17MJ0529-000188)

**b. “Interception of wire and electronic communications to and from any various and changing cellular telephones used by Arturo Gonzalez-Renteria.”**

- i. The government purportedly used this as authorization to monitor the following two telephones:

**4. “ROVING” – NO SPECIFIC ORDER OF AUTHORIZATION**

- a. **“5635 phone,” aka “TT#17(a)”;** (706-386-5635) – (Gonzalez-Renteria);
  - i. Interception Period: July 2, 2017 to July 13, 2017
  - ii. Return: July 14, 2017
  - iii. Sealing Order: July 14, 2017

**5. “ROVING” – NO SPECIFIC ORDER OF AUTHORIZATION**

- a. **“2847 phone,” aka “TT#17(b)”;** (714-357-2847) (Gonzalez-Renteria);
  - i. Interception Period: July 12, 2017 to August 10, 2017

- ii. Return: August 10, 2017
- iii. Sealing Order: August 10, 2017 (same return and sealing order as below)

**6. July 26, 2017 – CONTINUATION OF “ROVING” - 1:17-MJ-626**

- a. **“2847 phone,” aka TT#17b; (714-357-2847) (1<sup>st</sup> Cont.) (Gonzalez-Renteria) –**  
Made pursuant to the continued interception of 1:17-MJ-529 (TT#17 (470-449-5260))
  - i. Interception period (continuous from above): (beginning from July 12, 2017 purportedly pursuant to 1:17-MJ-529) and continuing July 26, 2017 to August 10, 2017 (1:17-MJ-626) (WIRE-17MJ0626-000185)
  - ii. Sealing Order: August 10, 2017
- b. **“Interception of wire and electronic communications to and from any various and changing cellular telephones used by Arturo Gonzalez-Renteria,”** which the government purportedly intended to use as authorization to monitor “any” future telephones used by Defendant.

As a result of these orders, Defendant’s wire and electronic communications were allegedly intercepted by law enforcement. Defendant believes that the Government is likely to introduce said interceptions against him at trial.

Defendant alleges the interception orders were illegal and his communications were illegally seized<sup>1</sup>) because the orders and the information supporting their probable-cause basis were the illegal fruit of the unlawful use of GPS tracking, *see Defendant’s First Particularized Motion to Suppress Evidence and Brief in Support “Part I”: Motion to Suppress Evidence Obtained from the Illegal Use of Global Positioning System or “GPS” Tracking (“Motion to Suppress ‘Part I’ ”)*, re-alleged and incorporated by reference herein, and 2) on the grounds alleged herein. *See infra*.

Also, law enforcement seized and/or obtained certain evidence, including evidence seized from his residence, which is the fruit derived not only from the illegal GPS tracking, but also the illegal wiretap interceptions. *See infra*. Because the intercepted communications supported orders to seize this evidence as the probable-cause basis, this evidence is the illegal fruit of the

unlawful wiretaps, as well as the fruit and derivative evidence of the illegal GPS tracking. *See Defendant's Motion to Suppress "Part I,"* re-alleged and incorporated by reference herein.

Therefore, all evidence obtained as a result of the illegal orders, and any derivative evidence, should be suppressed from evidence at trial.

Defendant expressly reserves the right to amend this motion in writing or *ore tenus* before this Court upon receipt of additional discovery, including discovery that his communications have been intercepted on any other telephones, and upon notification or discovery of any additional searches, seizures, or statements not described herein.

#### **E. Legal Basis for Challenge to the Title III Wiretap Orders**

**1. Probable Cause** - The communications were unlawfully intercepted and the wiretap orders were not supported by probable cause.

The affidavits for the wiretaps fail to provide probable cause for the issuance of the orders authorizing the wiretap interception, and were supported by stale and unreliable information. Through interceptions of Primo Siempre on TT6 and TT11, a Mexico-based phone number,<sup>8</sup> agents identified TT13 as being used by Defendant and alleged he was a money courier receiving drug related proceeds for Primo Siempre. (WIRE-17MJ0438-000047, -51, -55-56) Agents allegedly wanted to discover where Gonzalez-Renteria stored drug proceeds in Georgia and/or elsewhere and the methods used to transport bulk cash into Mexico. (WIRE-17MJ0438-000053) The initial affidavit for TT13 consists of allegations that Primo Siempre was giving Defendant's telephone numbers to other alleged conspirators to receive payment on his behalf. But despite the already unlimited access to GPS tracking to know every place Defendant was at

---

<sup>8</sup> The affiant stated that agents had not sought nor would seek approval to intercept Primo Siempre's Mexican telephone number, but would rather stick with the interception of the electronic messages through his BlackBerry application. (WIRE-17MJ0438-000071, n. 6)

any given moment, there is not single instance corroborating this information or that Defendant knew of or was connected to any transactions or stash locations. The affidavit relied on the GPS tracking to show that TT13 belonged to Defendant, and yet the GPS warrants were illegal as stated in *Defendant's Motion to Suppress Part I*, re-alleged and incorporated by reference herein.

As for subsequent applications and affidavits for Defendant's phones, and the extension orders, affiant relied on the same information provided in the initial order and the intercepted conversations and/or electronic messages obtained through the initial wiretap. Each subsequent affidavit would add information to the initial affidavit, which consisted of the wiretapped communications at issue. Additionally, because the subsequent wiretaps were invalid as the fruit of the initial illegal wiretap, all evidence obtained as a result should be suppressed from evidence at trial.

Therefore, because the wiretap orders were not supported by probable cause, all evidence obtained as a result of the wiretaps should be suppressed from evidence at trial.

**2. Necessity** - The applications and affidavits are invalid in that they did not contain sufficient probable cause and necessity for the wiretaps to issue. An application must establish probable cause for each such telephone. *See United States v. Carneiro*, 861 F.2d 1171, 1176-77 (9<sup>th</sup> Cir. 1988).

The "necessity" requirement of 2518(1)(c) and 2518(3)(c) – a separate and distinct requirement from the probable cause requirement – must be satisfied before a wiretap order may be lawfully issued. The purpose of the "necessity" requirement is "to ensure that the relatively intrusive device of wiretapping 'is not resorted to in situations where traditional investigative techniques would suffice to expose the crime.'" *United States v. Edwards*, 69 F.3d 419, 429 (10<sup>th</sup> Cir. 1995) (quoting *United States v. Kahn*, 415 U.S. 143, 153 n. 12, 94 S.Ct. 977, 983 (1974);

*United States v. Leavis*, 853 F.2d 215, 221 (4<sup>th</sup> Cir. 1988)(“The mere ‘boilerplate recitation of the difficulties of gather usable evidence’ cannot suffice”).

Prior to seeking a wiretap of Defendant’s phones, beginning on March 31, 2017, law enforcement sought and obtained numerous GPS tracking warrants which were not supported by probable cause and which were unconstitutional and invalid. *See Defendant’s Motion to Suppress Part I*, re-alleged and incorporated by reference herein.

Law enforcement also installed a pole camera outside Gonzalez-Renteria’s residence. Law enforcement conducted physical surveillance of Gonzalez-Renteria, took photos of him and his vehicles, obtained his driver’s license, and followed him for months wherever he went. Law enforcement also had numerous other on-going wiretap interceptions for other suspects, rendering the wiretap of his phone duplicative and unnecessary.

Therefore, the alleged difficulties that law enforcement had with present investigative techniques and in conducting an investigation without resorting to the wiretapping of Gonzalez-Renteria’s telephones is disingenuous.

Movant requests an evidentiary hearing regarding any assertion that the statutory requirements of 2518(1)(c) and (d) have been met. In light of the fact that other investigative techniques were in fact successful, as described below and re-alleged and incorporated herein by reference, the necessity requirement was not met.

**3. Failure to Show Other Investigative Techniques Failed** - The applications and orders are insufficient on their face in their failure to provide a sufficient showing that other investigative techniques have failed or why they reasonably appear to be unlikely to succeed if tried as required by 18 USC 2518(1)(c) and 18 USC 2518(3)(c).

Also, for the subsequent applications, law enforcement failed to make the requisite showing for continued surveillance. The affiant averred that “recent investigative techniques have not been successful in fully identifying all the TARGET SUBJECTS or in identifying all

the methods used to distribute drugs and collect drug proceeds....locations used to transport and/or store drugs and/or money generated from the distribution of the drugs, except as discussed herein...how this organization disseminates and divides the shipments to conspirators in Atlanta and elsewhere, or the system used to collect, count, and package drug proceeds, except as discussed herein. In this way, the requested interceptions are expected to help reveal the inner workings of this international drug trafficking organization.” (WIRE-17MJ0438-000075 to 000076) To summarize, the affiant averred that interception of TT13 was necessary “to uncover the full scope of this drug conspiracy, and that normal investigative techniques, without the support of court-authorized interception of communications over the Target Telephone, are reasonably unlikely to succeed and are, at times, too dangerous to employ.” (WIRE-17MJ0438-000128).

There is simply *no* normal investigation once the electronic surveillance commences. *United States v. Blackmon*, 273 F.3d 1204, 1209 (C.A. 9<sup>th</sup> Cir. 2001) (the statement “that the cooperating sources ‘only possess limited knowledge concerning the scope of the criminal enterprise’ ” is untrue and omits the extent to which the sources could have been used in gathering evidence against Blackmon).

The investigation of this case began in September of 2016. The affiant admitted that law enforcement had used numerous techniques proving successful during their investigation: physical surveillance, confidential informants/arrests and interviews, toll records, pen registers, pole surveillance, GPS or geo-location data, police reports/traffic stops and seizures, arrest records, grand jury and administrative subpoenas, and the prior wiretaps law enforcement had already executed or had under current surveillance.

The affidavits show that use of confidential informants, interviews of suspects, and the use of physical surveillance had been **successful**, not that it *failed*. The information derived from this was purportedly successful and was the primary basis for probable cause of the first wiretap.

Law enforcement had used current and historical pen register/toll record analysis, subscriber information, GPS tracking, and text/Blackberry messages with success.

Law enforcement had the capability to conduct traffic stops and surveillance of each suspect's movements outside of their residences due to physical surveillance capabilities available to law enforcement, and they did in fact utilize physical surveillance. Law enforcement identified the Defendant's and other suspects' residences, vehicles, and alleged stash locations prior to the wiretaps issuing. Law enforcement utilized certain investigative techniques like pole cameras and GPS tracking on Gonzalez-Renteria from the beginning of their investigation of him.

Therefore, the affidavit failed to make a sufficient showing that other investigative techniques had failed or why they reasonably appeared to be unlikely to succeed if tried as required by 18 USC 2518(1)(c) and 18 USC 2518(3)(c).

**4. Identity of Persons Whose Communications May be Intercepted** - The orders are invalid on their face in that they fail to specify the persons whose communications may be intercepted. 18 USC 2518(4). This requirement is separate and distinct from the requirements of 2518(1)(b)(iv)(requiring the *application* specify the identity of the persons known to be committing the offense) and 2518(3)(a)(requiring the Judge to find probable cause that an individual is committing a particular offense prior to entering a wiretap order).

Further, the orders authorized "background conversations" without specifying the particularities of the parties or persons to be intercepted. *See discussion, infra*. The orders *sub judice* fail to specify the identity of the persons whose communications may be intercepted on the targeted phones and how there is probable cause to intercept their communications on this particular phone. *See discussion supra*.

**5. Minimization** - Upon information and belief law enforcement agents failed to comply with the minimization requirement of 18 USC 2518(5).<sup>9</sup> Title III requires that the intercept order contain a provision that the interception shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception. 18 USC 2518(5) Under 18 U.S.C. §2517, “No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.” **The burden is on the Government to show proper minimization.** *United States v. Torres*, 908 F.2d 1417, 1423 (9<sup>th</sup> Cir. 1990); *United States v. Rizzo*, 491 F.2d 215, 217, n.7 (2<sup>nd</sup> Cir.), *cert. denied*, 416 U.S. 990 (1974). Pervasive and substantial failure to minimize non-pertinent calls as a whole allows the inference that the government engaged in an essentially warrantless, general search, warranting the suppression of all intercepted calls. *United States v. Suquet*, 547 F.Supp. 1034, 1037 (N.D. IL 1982); *See United States v. Blackmon*, 273 F.3d 1204 (C.A. 9<sup>th</sup> Cir. 2001). As such, this procedure did not meet the minimization requirements of Title III.

**6. Description of Communication to be Intercepted** - The applications and orders are insufficient on their face in their failure to provide a sufficiently particular description of the type of communication sought to be intercepted as required by 18 USC 2518(1)(b)(ii) and 18 USC 2518(4)(c).

The Orders provided authorization to not only intercept wire and electronic communications made on the Defendant’s phones between Defendant and others, but also authorization to seize “background conversations intercepted in the vicinity of any of the telephones used by Arturo Gonzalez while the telephones are off the hook or otherwise in use.”

---

<sup>9</sup> To date, it appears Defendant does not have discovery of law enforcement’s minimization of non-pertinent v. pertinent calls, nor does Defendant have discovery of the 15-day reports or the minimization training and sign-in sheets.

*See e.g.*, (WIRE-17MJ0474-000160); (WIRE-17MJ0626-000029 to -000030; -000172) (WIRE-17MJ0529-000031 to -000032; -000177)

This statement is vague, arbitrary, and authorized agents to potentially use Defendant's phones as listening devices when they were "off the hook," but still powered on, or "otherwise in use." This allowed law enforcement to potentially or actually intercept conversations not technically occurring on the phone, but "in the background" near the phone's vicinity, which would have violated Defendant's Fourth Amendment right to privacy in his home and his right to have privileged conversations without government intrusion. *See United States v. Olivia*, 705 F.3d 390 (9<sup>th</sup> Cir. 2012)(recognizing in the past the FBI has used a mobile phone's microphone to eavesdrop on nearby conversations; such terminology used is "problematical" and "ambiguous" which, if misconstrued, could "authorize interception of communications beyond what is intended," which would violate Title III's requirements for the authorizing order to be "clear and unambiguous...with respect to the use of the technology permitted and its boundaries."). *See* 2518(1); 2518(3)(c); 2518(4); *United States v. Jones*, 132 S. Ct. 945, 951 n.3, 181 L. Ed. 2d 911(2012) (Fourth Amendment analysis remains the same despite new methods of investigation); *Kyllo v. United States*, 533 U.S. 27, 36 (2001)(recognizing the effect of technology in relation to the Fourth Amendment).

The interception of telephones using a wiretap only involves interception of wire and electronic communications. Background conversations are not considered "wire" communications within the meaning of 18 USC 2510(1). *See* 18 USC 2510(1)("any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception") *and compare* 18 USC 2510(2) ("any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."). *See e.g., Company v. United States*, 349 F.3d

1132, 1139-39 (9<sup>th</sup> Cir. 2003); *United States v. Willoughby*, 860 F.2d 15, 22 (2d Cir. 1988); *see also United States v. Baranek*, 903 F.2 1068, 1070 (6<sup>th</sup> Cir. 1990)(government conceded wire communications were not the same as background communications).

18 U.S.C. 2511(1) prohibits the interception of oral communications except as provided in Title III, and further prohibits the use of evidence in violation of the statute. 18 U.S.C. 2515; *see also* 2518(10)(a)(iii) and (a)(i). Such a provision for “background conversations” rendered the wiretap orders illegal and insufficient on their face under 18 USC 2518(10)(a).

A hearing is also necessary to determine if the government relied on this language in the Orders and used the phones in this case, or any previous cases, to turn the phone into a listening device.

**7. Sealing** – the wiretaps were not sealed in accordance with 18 USC 2518(8)(a). That statute dictates that all interception recordings must be sealed “immediately upon the expiration of the period of the order” allowing the interceptions. In the absence of immediate sealing, the recordings must be suppressed, absent a satisfactory explanation from the Government stating not only why the delay occurred, but also why the delay is excusable. *United States v. Ojeda-Rios*, 495 U.S. 257, 265 (1990).

“Immediate” has not been defined as a certain number of days, but it is clear that sealing recordings within two days of expiration does satisfy 18 USC 2518(8). *United States v. Wong*, 40 F.3d 1347 (2d Cir. 1994) (two days with intervening holidays is immediate). *See also, United States v. Williams*, 124 F.3d 411 (3d Cir. 1997); *United States v. Wilkinson*, 53 F.3d 757 (6<sup>th</sup> Cir. 1995); *United States v. Pitera*, 5 F.3d 624 (2d Cir. 1993). Thirty-two days between expiration of the order and sealing, however, is not “immediate” in terms of the statute. *United States v. Jackson*, 207 F.3d 910, 915 (9<sup>th</sup> Cir. 2000).

Here, discovery indicates that the **5635 phone’s** last outgoing connected call occurred on **July 10, 2017** (Session 443). Beyond this call, all other calls appear to be non-connected

incoming calls with automated messages that continued until July 13, 2017.<sup>10</sup> Law enforcement did not obtain a sealing order for the calls until **July 14, 2017**.

For the **2748 phone**, the discovery indicates that law enforcement only intercepted communications between July 12, 2017 and **July 20, 2017** (Session 46). Despite any further indication the phone was being used, on July 26, 2017, law enforcement sought and obtained the first continued wiretap of the 2748 phone and another purported “roving” wiretap authorization for any other phone used by the Defendant. Beyond the July 20<sup>th</sup> call, the linesheets indicate that all other calls appear to be non-connected incoming calls with automated messages that continued until August 1, 2017, the date that the wiretap interception ceased altogether. The communications were not sealed by order of the court until **August 10, 2017**.

Therefore, the phones were not immediately sealed according to the requirements of 18 USC 2518(8)(a).

## **8. Territorial Jurisdiction of the Court**

Several telephones that were outside the issuing court’s territorial jurisdiction—and never entered the court’s jurisdiction—were intercepted in this case through the authorization of wiretap orders issued by judges sitting in the Northern District of Georgia. On October 25, 2016, the Honorable Mark H. Cohen, a U.S. District Judge for the Northern District of Georgia, authorized the first wiretap in this case for the interception of electronic communications over a Blackberry phone, TT1. (WIRE-17MJ0438-000120) The user was an individual known to live and stay in Mexico, “Servicio.” (WIRE-16MJ0882-000002) The issuing Court in the Northern District of Georgia did not have jurisdiction to issue an order to wiretap a phone located in Mexico. *See* 18 U.S.C. 2518(1), (3); *United States v. Glover*, 407 U.S. App. D.C. 189, 736 F.3d 509 (2013); *see discussion, infra*, re-alleged and incorporated by reference herein.

---

<sup>10</sup> It is unclear whether any of these calls were made by law enforcement, a fact to be determined at the hearing.

Because the orders for TT1 and the other telephones located in Mexico, including TT6 and TT11, belonging to “Primo Siempre,” (WIRE-17MJ0176-000007);(WIRE-17MJ0384-000010), were illegal and insufficient on their face, all subsequent wiretap orders for Defendant’s telephones were invalid as the fruit of the poisonous tree of the initial illegal orders. Further, because the evidence derived from these orders formed the probable cause basis to intercept Defendant’s telephones, *see e.g.* (WIRE-17MJ0438-000056 to -000066)(discussing interceptions of TT6 and TT11 as a probable cause basis to intercept Defendant’s TT13), all evidence derived from the interception of his phones should be suppressed from evidence at trial.

**F. The TT17 Wiretap Order, and the “Roving” Wiretap Interceptions were Illegal because the TT17 Order was Insufficient on its Face and the Issuing Court did not have Jurisdiction.**

On June 28, 2017, law enforcement submitted an “Application for Roving Interception of Wire and Electronic Communications,” which requested interception of Gonzalez-Renteria’s 470-449-5260 (“TT17”) telephone and “any various and changing cellular telephone” used by him pursuant to 18 USC 2518(11)(b), the “roving” wiretap provision of Title III. As a result, law enforcement used the TT17 order as authorization to seize the wire and electronic communications from his telephones 706-386-5635 and 714-357-2847 between July 2, 2017 – July 12, 2017, and July 12, 2017 - August 10, 2017, respectively.

**1. Law enforcement obtained TT17 by submitting an application made with reckless disregard for the truth, having material omissions, and made in bad faith.**

**a. Law enforcement sought a wiretap for a phone they knew was not in use.**

Law enforcement first obtained a GPS tracking order for Defendant’s telephone 470-449-5260 (“5260 phone”) on June 16, 2017. (1:17-MC-609) The seizure period for GPS tracking information was between June 16, 2017 and **June 27, 2017**. (GE0-17MC0609-000026);(WIRE-

17MJ0626-000066) Toll analysis<sup>11</sup> showed the “phone was in use for a total of 14 days,” from June 14<sup>th</sup> to June 27<sup>th</sup>. *Id.* Agents returned the GPS warrant to the Court on June 27, 2017.

Despite the fact agents *knew* the 5260 phone was no longer in use as of **June 27, 2017**. Law enforcement, nevertheless, submitted an application and affidavit, seeking (and obtaining) a wiretap for the 5260 phone (“TT17”) on **June 28, 2017**. (WIRE-17MJ0529-000001 to -000163)

An affidavit for a subsequent warrant (the continued interception of 2847 phone), confirms this fact, as the affiant averred, **“Based on pen register data and geo-location data from the 5260 phone, agents know that Gonzalez-Renteria stopped using the 5260 Phone on or about June 27, 2017.”** (Emphasis added.) (WIRE-17MJ0626-000068)

**b. Probable cause did not exist when a phone was no longer in use.**

18 USC 2518(3)(a), (b), and (d) require a finding of several probable cause determinations: (a) probable cause to believe that an individual is committing, has committed, or is about to commit a particular offense, (b) probable cause to believe that particular communications concerning that offense will be obtained through such interception, and (d) probable cause to believe that the facilities [or the phone] to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. *Id.*

The affiant averred that Gonzalez-Renteria “**is currently using 470-449-5260** (hereinafter ‘the Present Phone’),” (WIRE-17MJ0529-000051), and “hav[ing] been the user of TT#13, TT#15, and **now** the user of the Present Phone.” (Emphasis added.) (WIRE-17MJ0529-000056).

---

<sup>11</sup> Defendant has not received any discovery of pen register, toll records, subscriber records, and 15-day progress reports for any of the target phones. Therefore, Defendant reserves the right to amend this motion in writing or *ore tenus* before this Court upon receipt thereof.

The goals “for monitoring the Present Phone,” and “the original interception” of it and “any various and changing cellular telephone used by Gonzalez-Renteria,” included agents’ “hope to learn about the domestic operations of Primo Siempre’s organization, . . .to identify drug and money stash houses used by this organization . . . and learn about the existence and location of records related to the target subjects’ illegal activities.” (WIRE-17MJ0529-000059 to -000060) “There is probable cause to believe that Gonzalez-Renteria has used the prior phones and ***will use the Present Phone*** and any various and changing cellular telephone in a continued effort to engage in his illegal activities and to thwart law enforcement’s efforts to conduct electronic surveillance of such activity.” (WIRE-17MJ0529-000095)

The idea promoted that Defendant was still using the phone was perpetuated in a chart identifying “toll analysis” of the 5260 phone. The chart states that the Present Phone (5260 phone) was activated “6/14/17”; that the “First Call” occurred “6/14/17”; but that for the “**Last Call**,” the information was “N/A”; and the “**Total Days of Usage**” was “N/A.” (WIRE-17MJ0529-000096)

Part and parcel to any application is the requirement that the target phone identified is actually being used by the individual under investigation and is the phone law enforcement is seeking to intercept. *See id.* But in the case at hand, the alleged probable cause put forth in the application for the wiretap of 5260 phone was baseless and false, as agents knew Defendant was no longer using this phone. They had been using a pen register and GPS tracking for the phone. Through that, agents verified the phone was no longer being used by Defendant and submitted the return for the GPS warrant the day prior. Without the phone in operation, it was impossible for him to use it for any purpose, let alone for alleged criminal behavior. The phone was simply no longer in use prior to the law enforcement seeking a wiretap. The affidavit cannot support a

finding of probable cause without this material omission and/or false or misleading information, and therefore, the probable cause requirements of 18 USC 2518 were not met.

**c. A *Franks* hearing is required in this matter.**

Because the 5260 phone was no longer being used by Defendant, and this was a material fact necessary to the magistrate's probable cause determination, the application seeking a wiretap to intercept wire and electronic communications from TT17 and "any various and changing" phones, made a material omission and/or false or misleading statements to the court that were deliberately misleading, or made with reckless disregard for the truth and/or made in bad faith.

Once a substantial preliminary showing is made that 1) the government "knowingly and intentionally, or with reckless disregard for the truth" made a material omission or a false or misleading statement to the court, and 2) the affidavit cannot support a finding of probable cause without the allegedly false/misleading information/reckless omission of material facts, a defendant is entitled to a *Franks* hearing. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978).

"A warrant affidavit violates the Fourth Amendment when it contains omissions made intentionally or with a reckless disregard for the accuracy of the affidavit." *Madiwale v. Savaiko*, 117 F.3d 1321, 1326-27 (11th Cir. 1997) (citation and internal quotation marks omitted). "[E]ven intentional or reckless omissions will invalidate a warrant only if inclusion of the omitted facts would have prevented a finding of probable cause." *Id.* at 1327.

Defendant, therefore, requests a *Franks* hearing for the Court to determine whether the government misled the court in the event the Court does not first suppress all of evidence as stated herein.

**d. The fruit of the illegal wiretap should be suppressed.**

Because the purported probable cause to obtain a wiretap of the 5260 phone (TT17) served as the same alleged probable cause to seize additional phones 706-386-5635 (“5635 phone,” i.e., “TT17a”) and 714-357-2847 (“2847 phone,” i.e., “TT17b”) as “roving” wiretaps, any and all wire and electronic communications seized from these phones, and any evidence derived as a result, including evidence derived from subsequent orders and warrants, should be suppressed from evidence at trial as the fruit of the poisonous tree of the initial illegal wiretap. *See United States v. Giordano*, 416 U.S. 505, 94 S.Ct. 1820 (1974)(initial faulty wiretap invalidated the extension order and evidence derived from the extension order was tainted); *United States v. Spagnuolo*, 549 F.2d 705, 711 (9<sup>th</sup> Cir. 1977)(tainted evidence from the initial wiretap that was used as probable cause for the subsequent wiretap rendered the evidence from the subsequent wiretap tainted).

**2. The Issuing Court Did Not Have Jurisdiction**

**a. TT17 Order was the jurisdictional proxy to intercept more phones.**

Instead of any intention to actually intercept communications from the 5260 phone (TT17), agents sought a wiretap of it so that it could serve as a jurisdictional proxy to intercept any additional phones Defendant happened to use, including any phones first intercepted outside of the court’s jurisdiction, and the interception of phones regardless of whether they were actually connected to TT17 or met the requirements of 18 USC 2518(11). A closer look at these alleged “roving” phones shows that the Court did not in fact have jurisdiction over these phones.

First, the “Application for Roving Interception of Wire and Electronic Communications” (“TT17 Order”) requested interception of 470-449-5260 (“TT17”), “an AT&T cellular number,”

with International Mobile Subscriber Identity (“IMSI”) number “310410923625822, that is serviced through AT&T.” (WIRE-17MJ0529-000001, -10)

In addition, pursuant to 18 USC 2518(11)(b), the application sought authorization “for the original interception of wire and electronic communications occurring to and from any various and changing cellular telephone used by Gonzalez-Renteria during the thirty-day authorization period.” *Id.*

**b. The 5635 phone and the 2847 phone did not qualify as “roving” wiretaps.**

During the investigation, the government used the June 28, 2017, TT17 Order to act as legal authority to intercept any telephone Gonzalez-Renteria used after that point under the auspices of a “roving” wiretap. As a result, law enforcement intercepted the 5635 phone and 2847 phone.

**1) The 5635 phone was not initially intercepted in Georgia.**

As discussed in *Defendant’s Motion to Suppress, Part I*, re-alleged and incorporated by reference herein, law enforcement first obtained a GPS tracking warrant for the 5635 phone on July 1, 2017, but Defendant and the 5635 phone were physically located in the state of *Mississippi* at the time the warrant was issued at 5:33 p.m.<sup>12</sup>

Next, law enforcement first began the wiretap interception of the 5635 phone on **July 2, 2017**, which is a T-Mobile-assigned cellular telephone number. Based on GPS tracking “Gonzalez-Renteria was in the vicinity of Los Angeles, California on July 10, 2017. Specifically, geo-location data from the 5635 Phone showed that he had driven to Los Angeles.” (WIRE-17MJ0626-000080) GPS further showed he had been in California since July 7<sup>th</sup>. (DEA6-

---

<sup>12</sup> Law enforcement first learned of the 5635 phone through intercepted communications on TT#11 on July 1<sup>st</sup>, in which Primo Siempre allegedly gave the number to Rolex. (GE0-17MC0663-000015)

000299- 300) For the duration of the interception of 5635, GPS tracking indicated that Defendant was located in Texas and California.

**2) The 2847 phone was not initially intercepted in Georgia.**

On July 10, 2017, the 2847 phone was activated and the first call was made. (WIRE-17MJ0626-000078) The phone was a Verizon-assigned cellular telephone number.<sup>13</sup> On July 12, 2017, law enforcement began intercepting the 2847 phone, which is a phone “with an area code” that “encompasses an area that includes Los Angeles, California.” (WIRE-17MJ0626-000079-000080) Law enforcement identified this number “based on intercepted communications over the 5635 phone, geo-location data from the 5635 phone, and common contacts between the 5635 phone and the [2847 phone].” *Id.*

Thus, GPS tracking showed Gonzalez-Renteria was not located in Georgia at the time law enforcement first intercepted his communications on the 5635 phone or the 2847 phone.

**c. *United States v. Glover***

18 U.S.C. 2518(1) provides that each application for an order approving a wiretap “shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant’s authority to make such application.” 18 U.S.C. 2518(1). The jurisdictional provision of Title III is further found in 18 U.S.C. 2518(3), which states:

Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications ***within the territorial jurisdiction of the court in which the judge is sitting*** (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court ***within such jurisdiction***.” (Emphasis added.) 18 U.S.C. 2518(3).

---

<sup>13</sup> Discovery indicates that “no subscriber information is listed.” As stated above, Defendant has not received a copy of the subscriber information for this phone and reserves the right to amend this motion upon receipt thereof.

The Court in *United States v. Glover*, 407 U.S. App. D.C. 189, 736 F.3d 509 (2013), first held that in the parenthetical phrase of 18 U.S.C. 2518(3), the words “such jurisdiction” was reasonably interpreted as “referring back to the jurisdiction in which the judge is sitting,” and, “by implication, refers to the jurisdiction in which the mobile interception device is installed.” *Id.* at 194.

The Court explained, “Under either reading, the parenthetical makes clear that a judge cannot authorize the interception of communications if the mobile interception device was not validly authorized, and a device cannot be validly authorized *if, at the time the warrant is issued, the property on which the device is to be installed is not located in the authorizing judge’s jurisdiction*. A contrary reading would render the phrase ‘authorized by a Federal court within such jurisdiction’ completely superfluous.” (Emphasis added.) *Id.* The Court found that a Senate Judiciary Committee report confirmed the Court’s conclusion based on their objective “to ensure that warrants remain effective in the event a target vehicle is moved out of the issuing judge’s jurisdiction *after* a warrant is issued, but before a surveillance device can be placed in the vehicle.” (Emphasis in original.) *Id.*; *see* S. Rep. No. 99-541, at 106(a)(1986).

Rule 41 and Title III “impose the same geographic limitations on warrants to install listening devices,” and are therefore, “consistent.” *Id.* at 515. The Court in *Glover*, further held, “To the extent that there is uncertainty over the proper interpretation of the statute, Rule 41 of the Federal Rules of Criminal Procedure, which partially implements the statute, is crystal clear. It states that ‘a magistrate judge with authority *in the district* has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed.’ ” (Emphasis in original.) *Id.* (quoting Fed. R. Crim. P. 41(b)(2)).

The Court in *Glover* found that the warrant, therefore, appeared on its face to be in violation of the rule and the statute. *Id. See also Castillo v. State*, 810 S.W.2d 180, 183(Tex.Crim.App.1990) (because the Texas wiretap statute provided “only the judge of competent jurisdiction for the administrative judicial district in which the proposed interception will be made may act on an application,” territorial restrictions were established, and, therefore, “interception” did not occur at the listening post, but where the wiretap was physically placed or where the wiretap device is physically located).

Here, the phones at issue were not the same phone as the TT17. They were distinct phones with different service providers from TT17. Law enforcement did not determine these phone numbers existed and did not intercept them until several days after Defendant had left the state of Georgia. The Orders even indicate an understanding that the phones to be intercepted, both TT17 and “any various and changing cellular telephone” would be initially intercepted in the Northern District of Georgia, and that “in the event” these phones *left the territorial jurisdiction*, then continuing, roving interception outside of the jurisdictional territory could occur. The TT17 Order states:

IT IS FURTHER ORDERED THAT, *in the event* that the **Present Phone** and **any various and changing cellular telephone used by GONZALEZ-RENTERIA within the authorization period is transferred outside the territorial jurisdiction of this Court**, pursuant to Title 18, United States Code, Section 2518(3), wire and **electronic interceptions of the transferred facility may continue to take place** in the Northern District of Georgia, where all wire and electronic communications will first be heard/read and minimized. (Emphasis added.) (WIRE-17MJ0529-000177-000178); (WIRE-17MJ0626-000173).<sup>14</sup>

---

<sup>14</sup> The July 26, 2017, 2847 phone Order for continued interception and “any various and changing cellular telephone” contained the exact same provision. *Id.*

Because Congress provided a textual remedy of suppression when such evidence is gathered pursuant to a facially insufficient warrant, the *Leon* good faith exception does not apply in this case.

Therefore, because law enforcement did not begin interception of these phones until they were physically located outside of the issuing court's jurisdiction, the TT17 Order (and the subsequent July 26, 2017 Order) were insufficient on their face to authorize interception of the phones beyond the territorial jurisdiction of the issuing court, under 18 USC 2518(3).

#### **G. The “Roving” provisions of 18 USC 2518(11)(b) are Unconstitutional**

Title III requires that an application and order provide a “particular description of the nature and location of the facilities from which or the place where the communications is to be intercepted.” 18 USC 2518(1)(b)(ii). In conjunction with this provision, section 2518(3)(d) also requires a judge of competent jurisdiction to find that “there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.” 18 USC 2518(3)(d). These provisions that require specificity in the facilities to be intercepted, as well as a probable cause determination to support such interception, represent just one specification of the particularly requirements described and imposed by the statute. *See* 18 USC 2518(1), *et. al.*

In 1986, however, Congress enacted the Electronic Communications Privacy Act (“ECPA”) to address deficiencies in Title III. Congress expanded the definition of “wire communication,” and added “electronic communication,” to cover cellular telephones. 18 USC 2410(1), (12). Congress also enabled the government to circumvent this “particular description” requirement in the case, creating an exception when “the applicant makes a showing that there is

probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility." 18 USC 2518(1)(b)(ii), (11)(b)(II). The legislative history shows that the provision was, for example, intended to prevent an alleged terrorist from going from phone booth to phone booth numerous times to avoid interception, or, to allow interception in the case where the person whose communications were being intercepted stated that they planned to switch phones to avoid detection. S. Rep. 541, 99<sup>th</sup> Cong. 2d Sess. 32 (1986). But Congress recognized the dangers that roving wiretaps presented to privacy rights and enacted enhanced protections with the requirement for the application to be approved by a high-ranking Department of Justice official. 18 U.S.C. 2518(11)(b)(i). Particularity otherwise requires, at a minimum, that the phone number be specified. *See e.g., United States v. Goodwin*, 141 F.3d 394, 402-403 (2d Cir. 1997) (serial numbers and telephone numbers were identified in the affidavits).

In *Berger v. New York*, 388 U.S. 41(1967) and *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507 (1967), the Supreme Court recognized how intrusive wiretaps can be, and the protections in the Fourth Amendment that are available against electronic eavesdropping. By implementing Title III to incorporate the Fourth Amendment's expectation of privacy principles, Congress recognized society's expectation of privacy in one's wire, electronic, and oral communications. *See e.g.*, 18 U.S.C. 2511(1)(b)(making it illegal to intentionally "use any electronic, mechanical, or other device to intercept any oral communication" when the device is fixed to or otherwise transmits a signal through a wire or other connection or radio transmission).

If communications are intercepted in violation of Title III, "no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court." 18 U.S.C. § 2515. The statute therefore acts "parallel" to the reasonable expectation of privacy test described in *Berger* and *Katz* to ensure

that there is no abuse or misinterpretation of Fourth Amendment protections when law enforcement seek and obtain a wiretap. *See United States v. Larios*, 593 F.3d 82, 92 (1<sup>st</sup> Cir. 2010) (cits. omitted). *See also* 18 USC 2518(1)(b)(implementing the Fourth Amendment’s requirement to “particularly describe the place to be searched, and the ...things to be seized”).

A few courts have upheld the constitutionality of the roving provision. It is generally upheld based on the fact that a roving wiretap is only permitted if the person whose facilities are to be intercepted is identified and the government has established the person has attempted to evade surveillance. *See, e.g., United States v. Gaytan*, 74 F.3d 545 (5<sup>th</sup> Cir. 1996); *United States v. Petti*, 973 F.2d 1441 (9<sup>th</sup> Cir. 1992), *cert. denied*, 507 U.S. 1035, 123 L. Ed. 2d 480, 113 S. Ct. 1859 (1993); *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993).

But these cases fail to recognize that the authorization of the “roving” wiretap for unknown phones *ipso facto* allows the agents and law enforcement officials to make the determination *ex post facto* of whether the suspected phone actually belongs to the suspect. The “roving” provision of 2518(11) therefore violates the Fourth Amendment’s particularity requirement, in that a warrant must “particularly describ[e] the place to be searched.” U.S. Const. Amend. IV. *See e.g. Marron v. United States*, 275 U.S. 192 (1927) (“As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”). *See also, Groh v. Ramirez*, 540 U.S. 551 (2004)(a warrant that does not describe the items to be seized is “plainly invalid,” and particularity in supporting documents is insufficient if it is not cross-referenced in and accompanying the warrant). *United States v. Ellis*, 971 F.2d 701 (11<sup>th</sup> Cir. 1992)(warrant failed particularity test when it fails to adequately describe with particularity the place to be searched); *United States v. Clark*, 638 F.3d 89 (2d Cir. 2011)(when the warrant did not specify

which unit in a multi-family dwelling structure was to be searched, the warrant lacked probable cause to the extent it authorized a search of the entire building).

The roving wiretap authorizes a wiretap of “any telephone number” or serial number without requiring the government in the application and the order to first identify the place of interception. Law enforcement are permitted to wiretap *any telephone* based on their subjective or conclusory belief that a particular phone number may belong to the Defendant—which is determined *after* the roving wiretap is issued. The determination to intercept is therefore without judicial oversight.

The wiretap orders in this case fail to meet the particularity requirement of the Fourth Amendment and are unconstitutionally overbroad in application, which amounts to a general warrant.

#### **H. Evidence Obtained as the Fruit of the Illegal Wiretap**

In addition, as a direct result or derivative evidence of the illegal wiretaps, law enforcement sought and obtained certain evidence. For example, law enforcement sought and obtained search warrants, whereupon the information derived from the illegal wiretaps formed the basis for probable cause within the application and affidavits for the search warrants. Law enforcement searched and seized evidence from Defendant’s residence located at 4464 Jim Hood Road, in Gainesville, Georgia, which is the fruit derived from both the illegal GPS tracking and the illegal wiretap interceptions.

Because the search warrants/orders were the direct result of the information obtained from the wiretaps, the evidence seized as a result of the search warrants should be suppressed from evidence at trial as the fruit of the poisonous tree of the illegal wiretaps.

### I. No Good Faith Exception Under Title III

Further, the Court must examine the validity of the above wiretaps because there is no “good faith exception” for a warrant obtained pursuant to Title III. *United States v. Rice*, 478 F.3d 704, 711 (C.A. 6<sup>th</sup> Cir. 2007); *Glover, supra* (explicit textual requirement of suppression cannot be excused). *But see, United States v. Malekzadeh*, 855 F.2d 1492, 1497 (C.A. 11<sup>th</sup> Cir. 1988). The *Leon* exception does not apply when the warrant [or wiretap] is so overly broad that the executing officers could not have reasonably presumed it to be valid. *United States v. Travers*, 233 F.3d 1327 (11<sup>th</sup> Cir. 2000); *see also United States v. Rosa*, 626 F.3d 56 (2d Cir. 2010).

Therefore, any and all interceptions of Defendant’s wire or electronic communications in which he was the subject of the intercepted communications or a party to the intercepted communications should be suppressed from evidence at trial. Further, any evidence derived as a result of the illegal interceptions should be suppressed from evidence at trial.

WHEREFORE, Defendant respectfully requests this Court to grant an evidentiary hearing and to suppress any and all evidence improperly obtained against Defendant in this case. The Court should conduct a *Franks* hearing in the alternative.

Respectfully submitted this 6<sup>th</sup> day of March, 2018.

/s James R. Hodes

JAMES R. HODES, P.C.  
Attorney for Defendant

/s Bruce S. Harvey

BRUCE S. HARVEY  
Attorney for Defendant

**CERTIFICATE OF SERVICE**

I hereby certify that the foregoing document was electronically filed with the Clerk of the Court by using CM/ECF system, which will automatically send e-mail notification of such filing to the attorney(s) of record in the case, including opposing counsel.

Respectfully submitted this 6<sup>th</sup> day of March, 2018.

/s James R. Hodes

JAMES R. HODES

Attorney for Defendant

GA Bar #358647

Lead Attorney/Attorney to be Noticed

James R. Hodes, P.C.  
315 W. Ponce De Leon Avenue, Suite 1070  
Decatur, GA 30030  
(P) 404-513-9770  
(F) 855-710-6574  
jrhodes13@yahoo.com

/s Bruce S. Harvey

BRUCE S. HARVEY

Attorney for Defendant

GA Bar #335175

Lead Attorney/Attorney to be Noticed

LAW OFFICES OF BRUCE S. HARVEY  
146 Nassau Street, NW  
Atlanta, GA 30303  
(P) 404-659-4628  
bruce@bharveylawfirm.com